REMARKS:

This paper is herewith filed in response to the Examiner's final Office Action mailed on August 6, 2008 for the above-captioned U.S. Patent Application. This office action is a final rejection of claims 1-14 of the application.

More specifically, the Examiner has rejected claims 1-16 under 35 USC 103(a) as being unpatentable over Win (US6,453,353) in view of Wright (US20040123153). The Applicant respectfully traverses the rejections.

Claims 1, 7, 9, 13, 14, and16 have been amended for clarification. Support for the amendments can be found at least on page 8 line17 to page 10 line 3, and page 11 line 14 to page 12 line 8. No new matter is added.

Regarding the rejection of claim 1 the Applicant notes that claim 1 has been amended to recite:

> A method, comprising: performing an automated security scan of a second network device by a first network device to determine at least one of a hardware or software capability of the second network device; determining an attribute for the second network device based, in part, on the determined capability; generating an attribute certificate for the second network device based in part on the attribute; storing the attribute certificate including the attribute on a device other than the second network device; and responsive to a verified authentication request from the second network device for access to a resource over a network, determining whether the stored attribute certificate for the second network device is valid, where if the stored attribute certificate is determined valid, authorizing access to the resource over the network based, in part, on the attribute associated with the attribute certificate, or else denying access to the resource for the second network device.

Firstly, in regards to the rejection of claim 1 the Examiner states:

> "As to claims 1,14 and 16, Win teaches a method, comprising: performing an automated security scan of a second network device by a first network device to

> determine a capability of the second network device (line 8, col. 8, line 23-col. 9, line 40, col. 10, line 64-col. 12); generating an attribute certificate based in part on the attribute (col. 7, line 34-col. 8, line 46, col. 10, line 34-col. 11, line 9); storing the attribute certificate including the attribute (col. 6, line 20-65, col. 10, lines 14-67); and responsive to a verified authentication request, determining, that the attribute certificate is valid and authorizing access to a resource over a network based, in part, on the attribute associated with the attribute certificate (col. 9, line 14-col. 10, line 67, col.11, line 43-col. 12, line 8)."

As cited Win discloses:

> "Access Server 106 stores a log-in page, Authentication Client Module and Access Menu Module. The Authentication Client Module authenticates a user by verifying the name and password with the Registry Server 108. If the name and password are correct, the Authentication Client Module reads the user's roles from the Registry Server 108. It then encrypts and sends this information in a "cookie" to the user's browser. [...] A cookie returned by the Authentication Client Module is required for access to resources protected by the system 2," (emphasis added), (col. 6, lines 41-54).

The Applicants submits that Win can not be seen to be performing an automated security scan of a second network device to determine at least one of a hardware or software capability of the second network device as in claim 1. The Access Server 106 in Win is seen to be verifying a name and password with the Registry Server 108. The name and password which appears to be entered in the log-in page clearly can not be seen to disclose or suggest performing an automated security scan to determine at least one of a hardware or software capability of the device.

As cited Win discloses:

> "FIG. 3B is a state diagram showing processes carried out when the URL is a protected resource. As shown by state 312, Runtime Module 206 calls the Authentication Verification Service to check whether an authenticated user is making the request. An authenticated user is one who has successfully logged into the system. A user is considered authenticated if the request contains a "user cookie" that can be decrypted, and the request's IP address matches that in the cookie. If the conditions are not satisfied, then the user cannot be authenticated, and as shown in state 314, Runtime Module 206 returns a redirection to the Login URL. As shown by state 316, HTTP Server 202 returns the redirection to the Login URL to the browser 100," (emphasis added), (col.8, lines 23-35).

Here the Examiner appears to equate a "user cookie" in Win with an attribute certificate based in part on the attribute which has been determined based on a security scan determining at least one of a hardware or software capability of a network device as in claim 1. As similarly stated above, Win fails to disclose or suggest determining an attribute based, in part, on a determined at least one of a hardware or software capability of the network device. The "user cookie" in Win merely appears to be based on an accepted log-in at the Access Server 106. Thus, the "user cookie" of Win can not be seen to relate to an attribute certificate as in claim 1, where the attribute certificate for the second network device is based, in part, on the attribute.

Further, the Applicant notes that according to Win the "cookie" is stored in the browser of the device that has been authenticated. The Applicant submits that this is clearly distinguishable for where claim 1 recites "storing the attribute certificate including the attribute on a device other than the second network device." In addition, for at least the reasons already stated it clearly follows that Win can not be seen to disclose or suggest where claim 1 recites "responsive to a verified authentication request from the second network device for access to a resource over a network, determining whether the stored attribute certificate for the second network device is valid."

In addition, the Applicant submits that Wright, the additional reference cited against claim 1, can not be seen to address the above stated shortfalls of Win. Wright relates to a system for enforcing different security policies based on a location and different available security features of a mobile device. Wright uses a remote diagnostics module 224 in order to probe a particular client to verify its status and an authorization module 245 to establish communication with a mobile client to exchange security and diagnostics information (Abstract and pars. [0057]-[0059]). Wright is not seen to disclose or suggest at least where claim 1 relates to determining an attribute for the second network device based, in part, on the determined capability, generating an attribute certificate for the second network device based in part on the attribute, storing the attribute certificate including the attribute on a device other than the second network device, and responsive to a verified authentication request from the second network device for access to a resource over a network, determining whether the stored attribute certificate for the second

network device is valid.

For at least the reasons stated the Applicant contends that the references cited can not be seen to disclose or suggest claim 1 and the rejection of claim 1 should be removed.

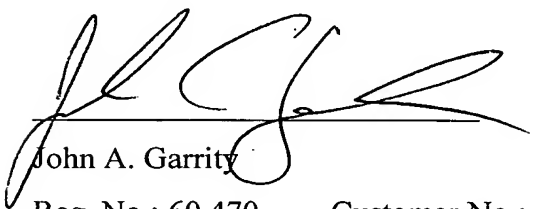
In addition, as the independent claims 9, 14, and 16 recite a feature similar to claim 1 as stated above, the references cited are not seen to disclose or suggest all claims 1, 9, 14, and 16. Therefore, the rejections of these claims should be removed.

Furthermore, for at least the reason that the claims 3-8; and 10 and 12-13; and 15; depend from claims 1, 9, and 14 respectively, the references cited are not seen to disclose or suggest these claims, and the rejections of all claims 1, 3-10, and 12-16 should be removed.

Based on the above explanations and arguments, it is clear that the references cited cannot be seen to disclose or suggest claims 1, 3-10, and 12-16. The Examiner is respectfully requested to reconsider and remove the rejections of claims 1, 3-10, and 12-16 and to allow all of the pending claims 1, 3-10, and 13-16 as presented for examination.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record. Should any unresolved issue remain, the Examiner is invited to call Applicants' agent at the telephone number indicated below.

Respectfully submitted:



12/4/08

John A. Garrity Date

Reg. No.: 60,470 Customer No.: 29683

HARRINGTON & SMITH, PC

S.N.: 10/823,378
Art Unit: 2153

4 Research Drive

Shelton, CT 06484-6212

Telephone: (203)925-9400

Facsimile: (203)944-0245

email: jgarrity@hspatent.com

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450.

12/4/2008 — Date

Elaine F. Muan — Name of Person Making Deposit